## AMENDMENTS TO THE CLAIMS

Claims 1, 2, 4, 5, 7, 8, 11, 12, 14, 17, 18, 21-27, 31, and 32 have been amended and claims 29 and 30 have been canceled. The following is a complete listing of the claims, which replaces all previous versions and listings of the claims.

1. (currently amended) A method of operating a first security module in a computer, the method comprising the acts of:

detecting a second security module in the computer;

determining whether a key associated with the second security module is stored at ~~available to~~ the first security module; and

obtaining the key associated with the second security module if the key associated with the second security module is not stored at ~~available to~~ the first security module.

2. (currently amended) The method set forth in claim 1, wherein ~~comprising the act of configuring~~ the first security module is ~~to be~~ a trusted platform module ("TPM").

3. (original) The method set forth in claim 1, comprising the act of requesting the key from the second security module.

4. (currently amended) The method set forth in claim 1, comprising the act of sending a public key from the first security module to the second security module if the key associated with the second security module is not stored at ~~available to~~ the first security module.

5. (currently amended) The method set forth in claim 1, comprising the act of sending a public key along with validation information from the first security module to the second security module if the key associated with the second security module is not stored at ~~available to~~ the first security module.

6. (original) The method set forth in claim 1, comprising the act of storing the key in a memory associated with the first security module.

7. (currently amended) The method set forth in claim 1, wherein ~~comprising the act of defining~~ the key is ~~to be~~ a private key.

8. (currently amended) A security module in a computer, comprising:

a detector that is adapted to detect another security module in the computer and determine whether one of a plurality of keys stored at the security module is associated with the other security module; and

a device that obtains at least one key associated with the other security module if the one of the plurality of keys stored at the security module is not associated with the other security module.

9. (original) The security module set forth in claim 8, wherein the security module comprises a trusted platform module ("TPM").

10. (original) The security module set forth in claim 8, wherein the security module is adapted to request the at least one key from the other security module.

11. (currently amended) The security module set forth in claim 8, wherein the security module is adapted to send a public key to the other security module if the at least one key is not stored at ~~available to~~ the security module.

12. (currently amended) The security module set forth in claim 8, wherein the security module is adapted to send a public key along with validation information to the other security module if the at least one key is not stored at ~~available to~~ the security module.

13. (original) The security module set forth in claim 8, wherein the at least one key is a private key.

14. (currently amended) A security module in a computer, comprising:

means for detecting another security module in the computer;

means for determining whether a key associated with the other security module is stored at ~~available to~~ the security module; and

means for obtaining the key associated with the other security module if the key associated with the other security module is not stored at ~~available to~~ the security module.

15. (original) The security module set forth in claim 14, wherein the security module comprises a trusted platform module ("TPM").

16. (original) The security module set forth in claim 14, wherein the security module is adapted to request the key from the other security module.

17. (currently amended) The security module set forth in claim 14, wherein the security module is adapted to send a public key to the other security module if the key associated with the other security module is not stored at ~~available to~~ the security module.

18. (currently amended) The security module set forth in claim 14, wherein the security module is adapted to send a public key along with validation information to the other security module if the key associated with the other security module is not stored at ~~available to~~ the security module.

19. (original) The security module set forth in claim 14, wherein the security module is adapted to store the key in a memory associated with the security module.

20. (original) The security module set forth in claim 14, wherein the key comprises a private key.

21. (currently amended) A computer ~~system~~ comprising:

a processor ~~for executing~~ configured to execute program instructions;

a storage device ~~for storing~~ configured to store program instructions to be delivered to the processor;

a first security module; and

a second security module ~~at least one peripheral device that is controlled by the processor;~~ ~~and~~

~~a first security module associated with the at least one peripheral device~~, the first security module comprising:

a detector ~~that is~~ adapted to detect ~~a~~ the second security module and determine whether one of a plurality of keys stored at the first security module is associated with the second security module~~; and~~, wherein the first security module ~~a device that~~ obtains at least one key associated with the second security module if ~~the~~ one of the plurality of keys stored at the first security module is not associated with the second security module.

22. (currently amended) The computer ~~system~~ set forth in claim 21, wherein the first security module comprises a trusted platform module ("TPM").

23. (currently amended) The computer ~~system~~ set forth in claim 21, wherein the first security module is adapted to request the at least one key from the second security module.

24. (currently amended) The computer ~~system~~ set forth in claim 21, wherein the first security module is adapted to send a public key to the second security module if the at least one key is not stored at ~~available to~~ the first security module.

25. (currently amended) The computer ~~system~~ set forth in claim 21, wherein the first security module is adapted to send a public key along with validation information to the second security module if the at least one key is not stored at ~~available to~~ the first security module.

26. (currently amended) The computer ~~system~~ set forth in claim 21, wherein the at least one key is a private key.

27. (currently amended) A method of unsealing information from a plurality of security modules, the method comprising the acts of:

detaching an identifier from sealed information for one of the plurality of security modules;

decrypting the sealed information with a key that is associated with another of the plurality of security modules;

calculating a hash of the decrypted sealed information; and

comparing the calculated hash to the identifier to determine if the key was used to encrypt the sealed information;

returning a decrypt key found message if the key is the key used to encrypt the sealed information or returning a decrypt key not found message if the key is not the key used to encrypt the sealed information.

28. (original) The method set forth in claim 27, wherein the plurality of security modules comprise trusted platform modules ("TPMs").

29-30. (canceled)

31. (currently amended) A computer network, comprising:

a plurality of computers ~~computer systems~~;

a network infrastructure that connects the plurality of computers ~~computer systems~~ together;

at least one of the plurality of computers ~~computer systems~~ comprising:

a first security module; and

a second security module, the first security module comprising ~~being configured to~~:

a detector adapted to detect the ~~a~~ second security module~~;~~ and determine whether a key associated with the second security module is stored at ~~available to~~ the first security module, ~~; and~~ wherein the first security module obtains ~~obtain~~ the key associated with the second

security module if the key associated with the second security module is not stored at ~~available to~~ the first security module.

32. (currently amended) The computer network, as set forth in claim 31, wherein the first security module ~~modules~~ comprises a trusted platform module ("TPM").